EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1311	380/30.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/08/08 13:15
L2	838	380/270.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/08/08 13:23
L3	884	713/156.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/08/08 13:16
L4	448	713/175.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/08/08 13:16
L5	1	(((personal security device) or card or PSD or token) and certificate and ((device name) or (serial number)) and seed and (public key) and (private key) and (shared secret key) and (attribut$4) and concatenat$4 and authenticat$4 and (key protection certificate)).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/08/08 13:28
S1	824	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 13:08
S2	457	713/193.ccls. and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:44
S3	2	(713/193.ccls. and @ad < "20010328") and ((Key near2 protect$3) with certificat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 14:10
S4	19	(713/193.ccls. and @ad < "20010328") and ((Key near2 protect$3) with (device or card or "serial Number" or serial))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 14:21

EAST Search History

S5	54	((key near2 instal$4) with certificat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 14:29
S6	29	(((key near2 instal$4) with certificat$3)) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 15:39
S7	206	(certificat$3 with (unaltered or unchanged or "manufacture near2 key" or right) with key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 15:42
S8	4	(((certificat$3 with (unaltered or unchanged or "manufacture near2 key" or right) with key)) and @ad < "20010328") and 713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/01 15:43
S9	86	((certificat$3 with (unaltered or unchanged or "manufacture near2 key" or right) with key)) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 08:22
S10	835	certif$4 with manufactur$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 08:23
S11	492	(certif$4 with manufactur$4) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 08:25
S12	492	(certif$4 with manufactur$4) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:18
S13	6	((certif$4 with manufactur$4) and @ad < "20010328") and 713/193. ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:18
S14	824	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:18

EAST Search History

S15	457	713/193.ccls. and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:18
S16	5	(713/193.ccls. and @ad < "20010328") and "key protect$"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:19
S17	5	(713/193.ccls. and @ad < "20010328") and "key protection"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 11:51
S18	0	(713/193.ccls. and @ad < "20010328") and ("key protection" with certificat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:18
S19	457	(713/193.ccls. and @ad < "20010328")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:19
S20	48	((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:20
S21	19	(((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:21
S22	2	((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:22
S23	1	((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and ("digital signature" with ("serial number" or identification))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:23

EAST Search History

S24	1	(((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and ("digital signature" with ("serial number" or identification))) and authenticat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 13:23
S25	2	(((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 16:26
S26	2	(((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 16:27
S27	2	((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and decrypt	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 16:27
S28	2	((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and decrypt$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 16:27
S29	2	(((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and decrypt$3) and symmetric	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 15:41

EAST Search History

S30	825	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 15:41
S31	458	713/193.ccls. and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 15:41
S32	252	("smart card" or SIM) with "serial number"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 15:42
S33	2	(713/193.ccls. and @ad < "20010328") and ("smart card" or SIM) with "serial number"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 16:32
S34	0	(713/193.ccls. and @ad < "20010328") and ("key protect$4 certificat$4")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 16:33
S35	0	(713/193.ccls. and @ad < "20010328") and ("key certificat$4")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 16:33
S36	33	(713/193.ccls. and @ad < "20010328") and (key near2 certificat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 16:33
S37	17	((713/193.ccls. and @ad < "20010328") and (key near2 certificat$4)) and "smart card"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/05 16:35
S38	9	(((713/193.ccls. and @ad < "20010328") and (key near2 certificat$4)) and "smart card") and ("data structure" or "data block" or "data packet")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:50
S39	319	"smart card" same ("serial number" or "device name")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:51

EAST Search History

S40	314	"smart card" same ("serial number")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:51
S41	156	("smart card" same ("serial number")) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:52
S42	33	(("smart card" same ("serial number")) and @ad < "20010328") and ("serial number" with (encrypt$3 or encipher$3 or scrambl$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:53
S43	0	((("smart card" same ("serial number")) and @ad < "20010328") and ("serial number" with (encrypt$3 or encipher$3 or scrambl$3))) and (("data block" or "data structure" or "data packet") with ("serial number" and "digital signature" and certificat$4))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:56
S44	0	((("smart card" same ("serial number")) and @ad < "20010328") and ("serial number" with (encrypt$3 or encipher$3 or scrambl$3))) and (("data block" or "data structure" or "data packet") with ("serial number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:56
S45	427	(("data block" or "data structure" or "data packet") with ("serial number"))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:57
S46	4	(("data block" or "data structure" or "data packet") with ("serial number" and certificat$))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/06 11:57
S47	1	((("data block" or "data structure" or "data packet") with ("serial number" and certificat$))) and ("serial number" with (encrypt$3 or encipher$3 or scrambl$3))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:43
S48	827	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:44

EAST Search History

S49	458	713/193.ccls. and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:48
S50	120	reject$3 near3 certificat$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:48
S51	66	(reject$3 near3 certificat$3) and @ad < "20010328"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 12:49
S52	2	"6209091".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 18:15
S53	2	"6189097".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 18:16
S54	2	"6005942".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/07 18:16
S55	2	(((((((713/193.ccls. and @ad < "20010328")) and ((symmetric or common) adj key)) and (key with certificat$3)) and ((encipher or cipher or encrypt$3) with ("data structure" or "data block" or "data packet"))) and "digital signature") and decrypt$3) and symmetric	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/04 16:28
S56	4653	certificat$3 near2 key	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 13:09
S57	30	certificat$3 near2 key near2 protect$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 13:16

EAST Search History

S58	2	"6005942".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 13:17
S59	18	("6005942").URPN.	USPAT	OR	ON	2005/05/17 13:31
S60	158	((device near2 key) near3 (authenticat$3 or verificat$3))	USPAT	OR	ON	2005/05/17 13:32
S61	29	((device near2 key) near3 (authenticat$3 or verificat$3)) same (signature or "digital signature" or certificat$3)	USPAT	OR	ON	2005/05/17 14:16
S62	4	(("device key") near3 (authenticat$3 or verificat$3)) same (signature or "digital signature" or certificat$3)	USPAT	OR	ON	2005/05/17 14:18
S63	20	(("device key") near3 (authenticat$3 or verificat$3))	USPAT	OR	ON	2005/05/17 14:23
S68	566	"key verification"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 14:26
S69	16	"key verification" same (device or card or SIM) same integrity	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/17 14:27
S70	6	("6209091" "6189097" "6005942"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/18 17:48
S71	2	"5623546".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/18 17:52
S72	2	"6751735".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/19 05:58

EAST Search History

S73	92	("5210795" "5204902" "5659616" "6367013" "6738912" "6823454" "6826690" "6061448" "6061448" "5825300" "6189096" "6256741" "5265164" "6148405" "5796841" "6134328" "6311218" "6615349" "6892302" "5701343" "6748531" "6233685" "6148404" "4868877" "5005200" "5214702" "5901227" "5958051" "5982898" "6385728" "6058383" "6212504" "6212504" "6230266" "5220604" "6202151" "6233341" "6310966" "6367009" "6601171" "6671804" "6742114" "6775782" "6789193" "5864667" "6111953" "5923756" "6198824" "6072876" "6085320").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/19 05:58
S75	2	ep-807911-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/04 15:20
S76	155	("hash value" or "message digest" or digest or "message authentiation code" or "MAC") same (compare or match) near9 ("serial number" or "serial No" or identifier)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/04 15:23
S77	19	("hash value" or "message digest" or digest or "message authentiation code" or "MAC") same (compare or match) near9 ("serial number" or "serial No")	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/04 16:46
S78	3	"4309569".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/05 06:57
S79	648	(decrypt$4 or decipher$4) same (compar$4) same (received) same (signature or digest or certificate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/05 06:59
S80	37	(decrypt$4 or decipher$4) same (compar$4) same (received near9 (identifier or identification)) same (signature or digest or certificate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/05 07:30

EAST Search History

S81	2	"6314521".pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/05 08:37
S82	2	ep-807911-$.did.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2006/01/05 08:37
S83	4237	KEY CERTIFICATE	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 15:57
S84	642	key near integrity	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 15:58
S85	288	key near integrity and ((digital signature) or certificate)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 16:10
S87	657037	integrated circuit	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 16:10
S88	0	(integrated circuit) same (key near5 protction near8 (certificate or signature))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 16:12
S89	195	(integrated circuit) same (key near5 (certificate or signature))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/22 16:20
S90	23	((integrated circuit) or (IC card)) near9 (generating near6 (key near5 (certificate or signature)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 12:01
S91	3	((integrated circuit) or (IC card)) near9 (generating near6 (key near5 (certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 12:03

EAST Search History

S92	451	(generating near6 (key near5 (certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 12:03
S93	132	(generating near6 (key near (certificate)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 12:03
S94	34	(generating near6 (key near (certificate))) and ((integrated circuit) or (IC card))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 13:08
S95	9	((integrated circuit) or (IC card)) near9 (generating near6 ((key near pair) or (public near private near key) or (asymmetric key)))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 15:20
S96	0	((integrated circuit) or (IC card)) same (generating near6 ((key near pair) or (public near private near key) or (asymmetric key))) same ((common or symmetric) near key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 15:23
S97	9	((integrated circuit) or (IC card)) and(generating near6 ((key near pair) or (public near private near key) or (asymmetric key))) same ((common or symmetric) near key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 15:23
S98	9	((integrated circuit) or (IC card)) and (generating near6 ((key near pair) or (public near private near key) or (asymmetric key))) same ((common or symmetric) near key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/01/23 15:23

Terms used:
personal security device or card or PSD or token and certificate and device name or serial number and seed and public key and private key and shared secret key and attribut$4 and concatenat$4 and authenticat$4 and

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200
Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relev

1 Equipping smart devices with public key signatures
Xuhua Ding, Daniele Mazzocchi, Gene Tsudik
February 2007 **ACM Transactions on Internet Technology (TOIT)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(274.64 KB) Additional Information: full citation, abstract, references, index terms

One of the major recent trends in computing has been towards so-called smart devices, such as PDAs, cell phones and sensors. tend to have a feature in common: limited computational capabilities and equally limited power, as most operate on batteries. T ill-suited for public key signatures. This article explores practical and conceptual implications of using Server-Aided Signatures (devices. SAS is a signature method that relies on partially-trusted serve ...

Keywords: Digital signatures, public key infrastructure

2 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing sys 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability t valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorize

3 Selected writings on computing: a personal perspective
Edsger W. Dijkstra
January 1982 Book
Publisher: Springer-Verlag New York, Inc.
Additional Information: full citation, abstract, references, cited by, index terms

Since the summer of 1973, when I became a Burroughs Research Fellow, my life has been very different from what it had been daily routine changed: instead of going to the University each day, where I used to spend most of my time in the company of o went there only one day a week and was most of the time that is, when not travelling!-- alone in my study. In my solitude, mai word in general became more and more important. The circumstance that my employe ...

4 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.03 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

5 General storage protection techniques: Securing distributed storage: challenges, techniques, and systems
Vishal Kher, Yongdae Kim
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press

Full text available: pdf(294.61 KB) Additional Information: full citation, abstract, references, index terms

The rapid increase of sensitive data and the growing number of government regulations that require longterm data retention ar have forced enterprises to pay serious attention to storage security. In this paper, we discuss important security issues related present a comprehensive survey of the security services provided by the existing storage systems. We cover a broad range of t security literature, present a critical review of the existing solutions, compare ...

Keywords: authorization, confidentiality, integrity, intrusion detection, privacy

6 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for sec scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support m use.We propose separating key management from file system security, letting the world share a single global file system no ma individuals manage keys. We present SFS, a secure file system that avoids internal ...

7 Securing wireless applications: ESCORT: a decentralized and localized access control system for mobile wireless acces domains

Jiejun Kong, Shirshanka Das, Edward Tsai, Mario Gerla

September 2003 **Proceedings of the 2003 ACM workshop on Wireless security WiSe '03**

Publisher: ACM Press

Full text available: pdf(401.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In this work we design and implement ESCORT, a *backward compatible*, *efficient*, and *secure* access control system, to facilitate access to secured wireless LANs. In mobile environments, a mobile guest may frequently roam into foreign domains while dema network services. ESCORT provides instant yet secure access to the mobile guest based on the concept of "*escort*", which refers network object with four distinct properties: (1) T ...

Keywords: decentralized access control, identity privacy, location privacy, mobile privacy, wireless security

8 Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS

Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas

November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**

Publisher: ACM Press

Full text available: pdf(447.59 KB) Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized appli would otherwise be prone to replay attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights mana In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine wit Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

9 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network desi analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physi and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-carc measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which th measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

10 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings

11 Security without identification: transaction systems to make big brother obsolete

David Chaum
October 1985 **Communications of the ACM**, Volume 28 Issue 10

Publisher: ACM Press
Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms, review

The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the secu individuals and organizations.

12 Protecting applications with transient authentication

Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '(**

Publisher: ACM Press
Full text available: pdf(294.40 KB) Additional Information: full citation, abstract, references, citing by

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identit change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously autl user's presence over a short-range, wireless link. We present the fo ...

13 Strong password-only authenticated key exchange

David P. Jablon
October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5

Publisher: ACM Press
Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods wh authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary at the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, alor preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

14 PP-trust-X: A system for privacy preserving trust negotiations

A. Squicciarini, E. Bertino, Elena Ferrari, F. Paci, B. Thuraisingham
July 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 3

Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, abstract, references, index terms

Trust negotiation is a promising approach for establishing trust in open systems, in which sensitive interactions may often occur entities with no prior knowledge of each other. Although, to date several trust negotiation systems have been proposed, none o address the problem of privacy preservation. Today, privacy is one of the major concerns of users when exchanging informatior Web and thus we believe that trust negotiation systems must effectively address pr ...

Keywords: Access control, attribute-based access control, automated trust negotiation, credentials, privacy, strategy

15 Identification control: Public key distribution through "cryptoIDs"

Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**

Publisher: ACM Press
Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this v fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each use *lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

16 Computer security (SEC): Efficient Diffie-Hellmann two-party key agreement protocols based on elliptic curves

Maurizio Adriano Strangio
March 2005 **Proceedings of the 2005 ACM symposium on Applied computing SAC '05**

Publisher: ACM Press
Full text available: pdf(234.27 KB) Additional Information: full citation, abstract, references, index terms

Key agreement protocols are of fundamental importance for ensuring the confidentiality of communications between two (or mc an insecure network. In this paper we review existing two-party protocols whose security rests upon the intractability of Diffie-H Discrete Logarithm problems over elliptic curve groups. In addition, we propose a new two-party mutual authenticated key agre and collectively evaluate the security and performance of all the schemes cons ...

Keywords: cryptography, elliptic curves, key agreement, protocols

17 Risk transparency: Privacy and security threat analysis of the federal employee personal identity verification (PIV) progra

Paul A. Karger
July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**

Publisher: ACM Press
Full text available: pdf(113.11 KB) Additional Information: full citation, abstract, references, index terms

This paper is a security and privacy threat analysis of new Federal Information Processing Standard for Personal Identity Verific 201). It identifies some problems with the standard, and it proposes solutions to those problems, using standardized cryptograp that are based on the Internet Key Exchange (IKE) protocol [16]. When the standard is viewed in the abstract, it seems to effe security and privacy, because it uses strong cryptographic algorithms. ...

Keywords: personal identification, privacy, smart cards

18 Protecting file systems with transient authentication

Mark D. Corner, Brian D. Noble
January 2005 **Wireless Networks**, Volume 11 Issue 1-2

Publisher: Kluwer Academic Publishers
Full text available: pdf(422.63 KB) Additional Information: full citation, abstract, references, index terms

Laptops are vulnerable to theft, greatly increasing the likelihood of exposing sensitive files. Unfortunately, storing data in a cryp system does not fully address this problem. Such systems ask the user to imbue them with long-term authority for decryption, authority can be used by anyone who physically possesses the machine. Forcing the user to frequently reestablish his identity is encouraging him to disable encryption.This tension between usability and secur ...

19 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research CASC**

Publisher: IBM Press
Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often u better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the applic experience, such tools display repeated occurrences of non-trivial commun ...

20 Formal analysis of card-based payment systems in mobile devices

Vijayakrishnan Pasupathinathan, Josef Pieprzyk, Huaxiong Wang, Joo Yeon Cho
January 2006 **Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54 ACSW**

Publisher: Australian Computer Society, Inc.
Full text available: pdf(199.95 KB) Additional Information: full citation, abstract, references, index terms

To provide card holder authentication while they are conducting an electronic transaction using mobile devices, VISA and Maste independently proposed two electronic payment protocols: Visa 3D Secure and MasterCard Secure Code. The protocols use pre- passwords to provide card holder authentication and Secure Socket Layer/ Transport Layer Security (SSL/TLS) for data confide wired networks and Wireless Transport Layer Security (WTLS) between a wireless device and a Wirel ...

Keywords: card-based systems, electronic payments, formal verification, mobile payment